SECRET

12 December 1978

MEMORANDUM FOR: All Community Security Group

SUBJECT: Revision of Compartmentation Programs

1.   The Office of Security, CIA completed an extensive review of the CIA Security Program following the Kampiles Case and made a series of recommendations which the DCI reviewed and made comments on. A copy of that paper is attached.

2.   Many of the recommendations have ramifications beyond the CIA. The DCI has directed the attention of [   ] Special Assistant to the DCI (tasked with revising the Intelligence Community's Compartmentation Programs), to three of them associated with information control security (nos. 14, 16, and 23). [   ] will consider these recommendations as he moves his Group toward implementation of approved compartmentation programs.

25X1

3.   Other recommendations could impact on some areas of interest to the Community Security Group. Among these are recommendations 13, 15, 17, 21, 22, and possibly 4 (as it relates to reinvestigation at the end of probationary periods for new employees), 5 (as it relates to requirements for policy of investigative coverage and 5 year reinvestigative coverage of Industrial Contractor employees), and 25 (as it pertains to Automatic Data Processing security requirements).

4.   I am concerned, lest CIA's recommendations have unseen Community ramifications. I request CSG members to review the OS recommendations and make appropriate comments on implications they see in them for the Community. I would appreciate having by 5 January your written observations with an outline of procedures or actions we might take (or have forced upon us) to permit us ensure Community equities in what CIA now views as a CIA program.

25X1

Attachment

Regraded UNCLASSIFIED
When Separated From
Attachment

This is an internal staff paper
and no further controls than
these required.
R. T.

78/183

Monday 11 Dec '78

Shows DCI margin notes

Office of Security Survey of CIA Security Program
SUMMARY OF RECOMMENDATIONS

Personnel Security

1. It is recommended that the current CIA Regulation

25X1 [ ] be revised to:

(a) Clearly charge individual supervisors in this Agency with basic responsibility for the security supervision of employees under their purview.

OK

(b) Require the appointment of <u>one or more Career Security Officers to each major Agency component</u> to assist Agency supervisors in fulfilling their security supervisory responsibilities.

OK - achieve by normal attrition one person per component & replace firm

(c) Charge Career Security Officers with the responsibility of selecting Designated Security Officers in each component who, as their subordinates, will assist them in fulfilling their responsibilities, and that their selection be concurred in by both the component head and the Director of Security.

I believe components should be; OS review & comment

(d) Require that each Designated Security Officer undergo an appropriate period of training in the Office of Security before he assumes his duties.

OK

(e) Include as the first two responsibilities of

the Career Security Officer:

(1) the establishment and maintenance of methods

for becoming aware of significant personnel

situations as a first priority; and

(2) the implementation of a CIA Security Awareness

Program, as developed by the Office of Security,

on a regular basis but no less than twice per

year.

DDCI upon rec of this

2, It is recommended that the ∧ Director of Security ~~be~~

~~authorized~~, in coordination with the heads of appropriate Agency

components, ~~to~~ determine where he wishes to have Career Area

Security Officers placed at Headquarters and in domestic and

foreign installations; after which appropriate action will be

taken to implement his determinations.

NOTE: Because of the time constraints placed upon the

authors of this report, it is not possible at this

time to state precisely how many new Career Security

Officer positions would be required to implement

this program. *Same technique as 1 (8)*

3. It is recommended that a new group be established and

properly staffed within the OS to include all indoctrination

and education functions, patterned after the program in

OK

SECRET

existence at NSA. The functions of the new group would
include: EOD and exit briefings; serving as a focal point
for consultation and channeling personnel problems to the
proper components; guidance to employees regarding outside
activities; briefings and debriefings prior to PCS/TDY over-
seas assignments, private travel and access to sensitive
compartmented information; the establishment of an on-going
security awareness program.

Presuming that some existing resources could be
reallocated in establishing this group, it is estimated that
approximately four to six new positions would be required to
achieve comparability with the NSA program.

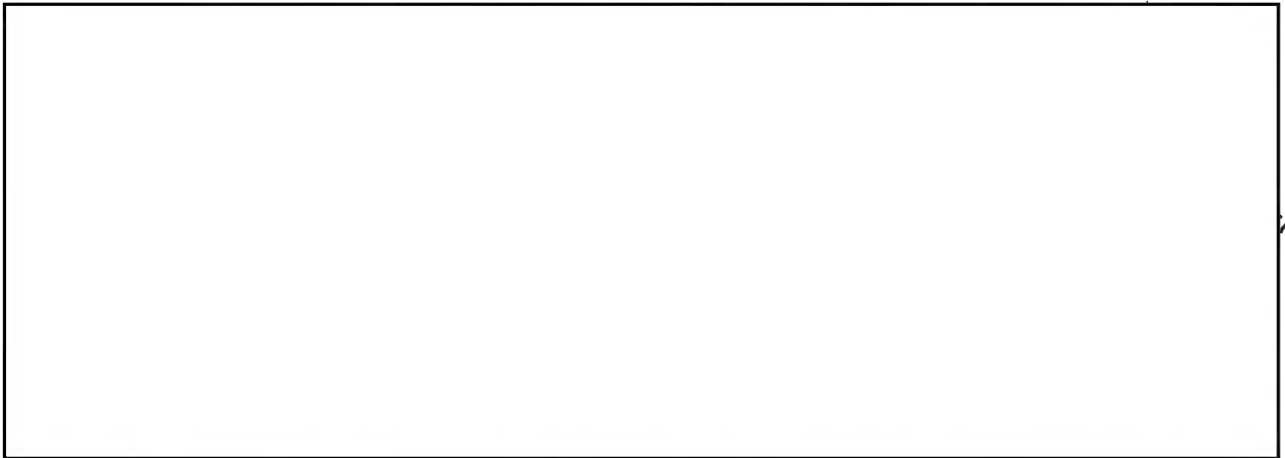*Do wth existing assets. DDCI to review + 4-6 in late budget decision*

4. It is recommended that probationary employees be
screened prior to becoming career employees by a combined
review by their Career Service, OMS, OS, and OP. Such screen-
ing would include a review of fitness reports and supervisory
comments and the recommendation of the Career Service and OP,
an updating and review of medical records, and a reinvesti-
gation and EOD-type polygraph by OS. It is anticipated that
this recommendation would require additional personnel
resources in OS, OMS, and OP. *OK but w/in existing resources*

5. It is recommended that a policy be adopted requiring
that Industrial Contractor employees undergo an investigation

SECRET

6. It is recommended that a minimum of six additional
field agents and one case supervisor be approved to handle
approximately 2,800 additional cases annually.

Physical Security

7. In order to obtain a desired degree of compound access
control, Gate #2 (West Lot) and Gate #3 (George Washington
Parkway) should be restricted to badged employees only. All
unbadged entry should be directed to Gate #1 (Route 123) where
a visitor processing area would be developed. This area, to
the right of Gate #1, should be examined by a traffic-design
consultant in order to effect the desired level of control
without significantly hindering the conduct of official
business. The ultimate solution for this area should take
into account the need to verify an individual's stated purpose
for visiting the Agency. The processing area should be capable
of handling, with an acceptable level of inconvenience, all

SECRET

categories of unbadged visitors. Special parking areas would be required in the immediate area and consideration should be given to a compound shuttle bus system to bring visitors to the Main Entrance after initial screening. Additionally, the use of temporary and permanent vehicle passes to facilitate the passage of frequent visitors should be considered during this study.
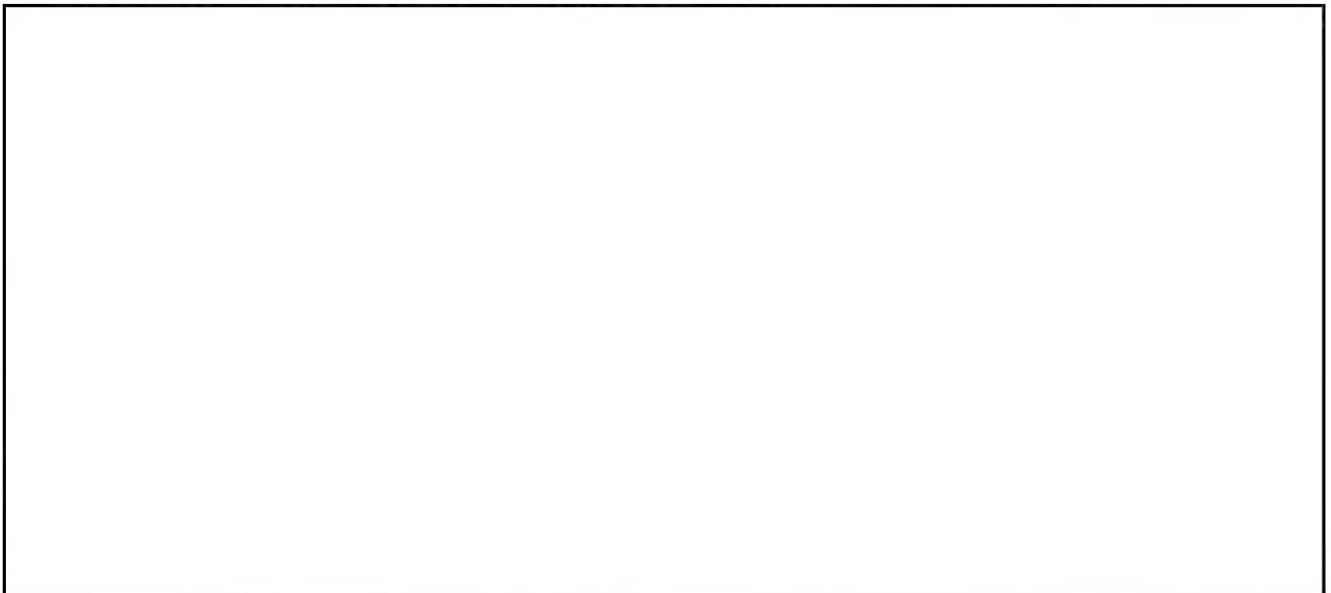
OK

25X1

25X1

OK

10. It is recommended that a complete review of all VNE badge holders be undertaken with the respective sponsoring offices. Procedural constraints on VNE badge issuance, such as sponsoring office justification memoranda and Office of Security review mechanisms, should be reassessed and significantly modified. The continuing responsibility of a sponsoring individual for a VNE badge holder must be clearly

OK

Plus – ZBB review all VNE badges; delete all non-US personnel; reduce total by at least 50%.

90

SECRET

established and accepted. The reviewing role of the Office of Security must be affirmed and exercised. The categories of individuals presently holding VNE badges should be scrutinized, and any inappropriate category, such as IBM or Xerox maintenance personnel, changed to a proper badge.

25X1

12. It is recommended that CIA institute a program for the selective and progressive elimination of all obsolete security container safe files from the Agency's inventory, beginning with those currently located at Agency facilities outside of the Headquarters Building. This should be funded by the Office of Logistics and carried out in an MBO format.

Information Control Security

13. It is recommended that the DCI appoint an action group to define precisely which intelligence requires TOP SECRET classification, both within and outside the compartmentation systems, and provide specific, detailed guidance

SECRET

with the intent of reserving TOP SECRET classification for
information of truly extraordinary sensitivity and imposing
strict accountability and rigid physical security upon
those items determined to be TOP SECRET, both collateral
and SCI.

OK

25X1

14. It is recommended that strict accountability be
imposed upon TOP SECRET SCI materials, identical to that
required for noncompartmented TOP SECRET, but within compart-
mented channels. This should include TOP SECRET SCI electrical
message traffic.

15. It is recommended that a zero-based review of the
dissemination of sensitive intelligence reports and publications
be conducted, to ensure that all subscribers have a true need
for the materials they receive. It is further recommended
that revalidation of these requirements be provided in January
of each year, with approval certified first at the Branch and
then at the Division level of the originating office. User
profiles should be superimposed on the distribution of all
intelligence publications to provide a need-to-know filter
limiting the individual's topical access. Pre-printed covers
for intelligence publications should reflect the actual clas-
sification and compartmentation of the material they cover.

OK

16. It is recommended that procedures be established to
permit readers to challenge serious anomalies in classification

SECRET

SECRET

25X1

or compartmentation, requiring prompt reevaluation and
response by the originator.

17. It is recommended that an intensive review of
current registry operations, policies, procedures and
requirements be undertaken.

18. It is recommended that the responsibility for
policy and procedural guidance of basic registry functions
be removed from the individual components and placed under
central authority.

19. It is recommended that formal training in security
document control procedures be made mandatory for all
registry personnel and others assigned responsibility for
controlling sensitive documents.

20. It is recommended that a career service be created
to include all registry officers and information control
specialists.

21. It is recommended that all office copiers and micro-
form printers be located in registries or document control
centers, to be operated only by information control specialists
who will ensure that all copies of controlled documents are
properly registered, controlled and stored.

22. It is recommended that all controlled documents
(TOP SECRET, SCI, etc.) be transmitted only from registry

SECRET

SECRET

to registry, and that they be controlled and held in registry
reading rooms, where they may be read by those requiring   *OK*
access.   In fully justified cases, controlled documents
might be charged out to individuals for brief periods, with
prompt follow-up on documents not promptly returned.

23.   To supplement Executive Order 12065, it is recommended
that TOP SECRET intelligence documents, once defined as recom-
mended previously, be inventoried annually, whether SCI or non-
SCI.   All Intelligence Community elements should initiate an
ongoing program to spot-inventory controlled documents, whether
held by individuals, components, or registries.

24.   It is recommended that the Office of Security create
a unit to conduct security audits of Agency components, similar
to the recently-instituted Industrial Security Audits.   This
unit should also conduct spot inspections of controlled docu-
ment holdings whether they be accountable to individuals,
components, or registries.

25.   It is recommended that security requirements be
included in ODP standards to enhance security control of
classified data by need-to-know profiles for topical access to
data; by utilizing user codes and ID numbers to access data;
by creating audit trails for all data output, and by applying
classifications, copy numbers and other controls to data output.
It is further recommended that all Agency ADP systems be designed
in accordance with ODP programming and production standards.

SECRET

SECRET

(

26. It is recommended that a CIA component be given the responsibility to monitor technological advances in the ADP field for the eventual development of a central, formalized computer-operated document accountability system for registry use and for use at remote terminals.

?

DDCI

SECRET